Challenges of Sending Large Files Over Public Internet

JONATHAN SOLOMON
SENIOR SALES & SYSTEM ENGINEER, ASPERA, INC.
Setting the Stage (How old is the technology you’re using today?)
What is TCP (and why doesn’t it work well?)
Ways to moving things faster
Features to look for
Network Security 101
Q&A
1972
SETTING THE STAGE

1984
SETTING THE STAGE

1984
SETTING THE STAGE

1986
SETTING THE STAGE

1982
WHAT DO THEY ALL HAVE IN COMMON?

- Were new technologies.
- Were the best at the time.
- Had wide acceptance.
- Allowed growth into newer technologies.
- Had awesome cars and suits.
- At the time, nobody could beat them.
Are any of them still useful?

If you could, would you still want to use any of them?

So why is TCP still used?
HOW DO I KNOW IF I AM USING TCP TO TRANSFER FILES?

• TCP file transfers include the following:
  • FTP
  • SCP
  • HTTP(S)
• Non-commercial sharing sites (Box.net, Google Drive, etc)
• Some commercial sharing services
• Windows Shares (\server\share)
Data Size and Volume
- Today’s “Drive,” “File Sync” and “File Sharing” services are impractical for Big Data
- Large data sets (large files or large collections of files) cannot move

Speed and Performance at Distance
- On global WANs (100 millisecond RTT / 1% packet loss+) standard TCP rates are <<10Mbps
- Transfers and sync sessions are extremely slow and most often do not complete at all

Security
- Security for hosted solutions is dependent on security of the provider
- Access control is limited and integrity of file ownership is fragile, with huge concerns over privacy,

Deployment Options
- Typical SaaS offerings don’t support on premise or hybrid infrastructure
- Often a single infrastructure solution

Sharing Paradigms
- Users are typically locked into a single delivery option
- Sync, Share, or Person-to-Person delivery

Compliance, Auditing and Control
- Limited controls, lack of visibility into risk, weak compliance auditing tools
‘Big’ Data Explosion & Almost All Media is File Based

- 90% of data today file-based or unstructured
- Mix of file sizes—but larger and larger files, and ever higher resolution are the norm
- From 20/80 to 80/20 “file/tape” in one year

Diversity of IP Networks—Media, Bandwidth Rates, and Conditions

- Variable bandwidth rates (slow to super-fast)
- Bandwidth rates increasing—costs decreasing
- Network media remains diverse (terrestrial, satellite, wireless)
- Conditions vary—all networks prone to degradation over distance

Global Live and “Near Live” Experiences are Expected

- World Cup and Olympics have explosive growth in online streaming audiences (web and mobile)
- Over distance, network conditions degrade and contemporary TCP based streaming solutions degrade
- CDNs considered essential for distribution
- Dedicated satellite feeds traditionally essential for live ingest of broadcast quality

Cloud Computing Grows Up

- Enterprises are moving core business workflows to the cloud
- No longer a niche – Netflix (transcoding), Sony CI, MLB, FIFA World Cup, etc.
TCP Performs well under ideal conditions
  • Low latency and low packet loss typical of LAN

TCP performance degrades with distance
  • Throughput bottleneck becomes more severe with increased latency and packet loss

TCP does not scale with bandwidth
  • TCP designed for low bandwidth
  • Adding more bandwidth does not improve throughput

Alternative technologies offer limited benefits
  • Modified TCP – Improves TCP performance but insufficient for fast networks
  • Data caching - Inappropriate for many large file transfer workflows
  • Data compression - Time consuming and impractical for certain file types
  • CDNs & co-lo build outs - High overhead and expensive to scale
GOODPUT

- **throughput** = the rate of successful message delivery by the network

- **goodput** = the rate of useful information delivery by the network

- All overhead reduces goodput:
  - retransmitted packets due to router buffer overflow
  - retransmitted packets due to storage buffer overflow
  - retransmitted packets due to packet loss

- Goal: maximize goodput by minimizing the amount of redundant data on the network

- An optimal system will maximize goodput
The laws of physics limit the speed at which light and electromagnetic signals can travel. Between any two endpoints it will take some time for the data to make a traversal. This is called latency, and Round Trip Time (RTT) is the time it takes to go someplace and back (one round trip).
TCP - LATENCY

Latency increases with distance

The longer the distance, the higher the latency, and the more TCP packets that might be sent before a SEND-ACK is received by the sender.
TCP Sliding Window

The amount of data that is sent but unacknowledged. This value is set by the Congestion Control and Flow Control algorithms.

The optimal sliding window size is a value close to the Bandwidth Delay Product.

Flow Control

This is to ensure reliable delivery of packets in order.

Congestion Control

Packet loss imposes additional limits to throughput. Packet loss or ACK loss detected by the sender causes the sender to reduce the send window to 1/2 or 0.
TCP – GOOD NETWORK (LAN)

All networks have some form of packet loss. When a packet is dropped, TCP resets the send window. After the data starts to flow again, it has a ramp up period.

When latency and packet loss are low, TCP performs well.
TCP – BAD NETWORK (SAWTOOTH)

TCP sawtooth pattern in poor conditions

When latency and packet loss are high, constant resets of the sliding window mean that TCP never has a chance to achieve high bandwidth.
NON TCP TRANSFERS

Bandwidth

Time

Packet Drops
Between two endpoints the latency is physically fixed at a lower bound that cannot be made faster, but that is not the whole story.

As routers and other devices that process packets get busier, the buffers and queues they maintain fill up. It takes longer and longer to process packets, and this can mean an increase in the observed latency.

Thus, these increases in observed latency are indicative of queuing.

A router can get so busy that it can no longer handle new packets, the buffers fill up, and packets are dropped.
Even a single slow router can affect end-to-end throughput.
ISP BANDWIDTH VS AVAILABLE BANDWIDTH

- Physical Capacity
- Storage Write Rate

Bandwidth vs. Time
ISP BANDWIDTH VS AVAILABLE BANDWIDTH
<table>
<thead>
<tr>
<th>ISP BANDWIDTH VS AVAILABLE BANDWIDTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
</tr>
<tr>
<td>Bandwidth</td>
</tr>
<tr>
<td>Physical Capacity</td>
</tr>
<tr>
<td>Storage Write Rate</td>
</tr>
<tr>
<td>License</td>
</tr>
<tr>
<td>Target Rate</td>
</tr>
<tr>
<td>(Client bandwidth cap)</td>
</tr>
<tr>
<td>Server bandwidth cap</td>
</tr>
<tr>
<td>Vlink</td>
</tr>
</tbody>
</table>

Diagram showing bandwidth over time with various metrics.
ISP BANDWIDTH VS AVAILABLE BANDWIDTH

The lowest maximum wins
TCP VS ALTERNATIVE

- Storage Write Rate
- Client / server b/w cap
- Physical Cap / License
- Available network bandwidth
- TCP performance

Time

Bandwidth
TCP VS ALTERNATIVE
<table>
<thead>
<tr>
<th>Time</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP performance</td>
<td>Available network bandwidth</td>
</tr>
<tr>
<td></td>
<td>Physical Cap / License</td>
</tr>
<tr>
<td></td>
<td>Storage Write Rate</td>
</tr>
<tr>
<td></td>
<td>Client / server b/w cap</td>
</tr>
</tbody>
</table>

**TCP VS ALTERNATIVE**
WAN Accelerators

- In line product
- Often used between two offices
- Good for file shares & email
- Caches data for quicker access
- No real file acceleration on “fresh” content
Enterprise Files Sync & Share (EFSS)

- Web GUI based
- Often used for Group Sharing
- Uses HTTP (TCP)
- Limited to no file acceleration

Watch out for:

- Security
- Audit Trail
- Control of content (may be on users personal computer or phone)
- File Size (or total size) limitations
UDP “Blasters”

As the name implies, blasts data via UDP and sees what ‘sticks’.

• Excessive retransmissions

Watch out for:

• Integration into your systems/workflow (API)
• Resource utilization (CPU and NIC)
• Congestion Avoidance
• Write to cloud (most require cache/local write to appliance before copy to disk)
UDP Transfer Products

- Usually Proprietary protocol (open source does exist)
- Server/Client model
- Improved performance

Watch out for:

- File limitations
- Network Limitations
- Integration into your systems/workflow (API)
- Resource utilization (CPU and NIC)
- Congestion Avoidance
- Write to cloud (most require cache/local write to appliance before copy to disk)
Other Solutions

- FedEx (HDD, HDCam, LTO, etc)
  - Reliable, but high latency
- “Baseband” TX (satellite, fiber)
- Dark Fiber
The following are software features to consider:

- Security
- Adaptable (bit rate)
- Line speed, congestion, disk speed management
- Management and control
- Minimum overhead
- Minimum retransmission
- Scalability / Clustering
- Uniform look across OS (even mobile)
- Customer Support
- Cloud Support and integration
- In line QC (Anti-virus/File Validation)
- DAM/MAM Integration
Passwords

- Change equipment default passwords as soon as you open the box!
- Maintain a secure enterprise password directory (if needed).
- Use complex passwords (uPP3r&L0weRc@s5+Sym8olz!) [>12 characters].
- Avoid passwords that spell something even when complex, especially on edge equipment.
- Change passwords every 90 days (or less).
- Have a plan for when a power user with password access leaves the company.
- If you need to, writing passwords on a piece of paper is more secure than in a file on your computer (or worse, company share). Don’t associate it with the user name.
Networks

- **USE A FIREWALL.** A good one. That is properly setup.
- Close down all incoming ports that are not needed. Log each exception ("pin hole").
- Regularly check server and network logs for suspicious activity.
- Maintain two networks when possible: a closed "production" network and an internet accessible "corporate" network.
- Use a DMZ when needed.
- Do not dual home machines (two network connections).
- Use email and attachments scanning, and scan all files going between networks.
- If possible use IDS (Intrusion Detection Systems).
**Personnel**

- Training, Training, Training!
- Do NOT share passwords. Ever.
- Do not EVER EVER EVER EVER open an attachment or link that you are not 100% certain is safe.
- Support does not randomly call you. Ever. That’s what Sales folks are for!
- A website will never ask you to verify your account through an email.
FILE DELIVERY Q&A

?? ANY

?? QUESTION

?? ??
Thank you

Visit us online at www.asperasoft.com
Reach me at jsolomon@asperasoft.com